UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/911,042	07/23/2001	Takumi Okaue	SONYJP 3.0-190	3744

530	7590	01/04/2005	

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER
POPHAM, JEFFREY D

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-24* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-24* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *23 July 2001* is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☒ All   b) ☐ Some *   c) ☐ None of:

   1. ☒ Certified copies of the priority documents have been received.

   2. ☐ Certified copies of the priority documents have been received in Application No. _____.

   3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20040202, 20041115*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claims 1-24 are pending

Claim Objections

1.   Claims 1, 6, 7, 10, and 11 are objected to under 37 CFR 1.75(a) because

of the following informalities:

-        Claim 1, lines 3 and 6 recite the limitation "said data processing

device". There is insufficient antecedent basis for this limitation in

the claims. It has been assumed to be "said data processing

apparatus" for purposed of prior art rejections.

-        Claim 6, line 7 recites the limitation "said individual data processing

apparatuses". There is insufficient antecedent basis for this

limitation in the claims.

-        Claim 7, line 4: "such path" should be "such paths".

-        Claim 10, line 8: "key also include" should be "key also includes".

-        Claim 11, line 8: "comprise such" should be "comprises such".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described
as set forth in section 102 of this title, if the differences between the subject matter sought to
be patented and the prior art are such that the subject matter as a whole would have been
obvious at the time the invention was made to a person having ordinary skill in the art to which

said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1, 8, 12, 13, 20, and 24 are rejected under 35 U.S.C. 103(a) as

being unpatentable over "Key Technology for Digital Content: Memory Stick

Copyright Protection Technology – MagicGate –", CX-NEWS Vol. 20, 05/2000

(hereinafter referred to as MGPUB) in view of Lin (U.S. Patent Application

Publication 2002 0,025,046).

Regarding Claim 1,

MGPUB discloses the following:

A data processing apparatus [memory stick walkman] for

executing reproduction of data from a memory device [memory

stick] or for recording of data into a memory device; wherein

The data processing apparatus has a structure for executing

reproduction of data from the memory device or recording of data

into the memory device on condition that a mutual authentication

between the data processing apparatus and the memory device is

established (Page 2, Paragraph 1, lines 8-10).

MGPUB does not disclose the use of a virtual memory

device.

Lin, however, discloses that mutual authentication will take

place between a proxy emulating the memory device and the data

processing apparatus in the case when the memory device has no

function to execute the processing for mutual authentication

(Detailed Description, Paragraph 0021, lines 4-14). This new

system would be the system of MGPUB mutually authenticating the

data processing device with a proxy acting on behalf of the memory

device.

It would have been obvious to one of ordinary skill in the art

at the time of applicant's invention to use a proxy to emulate the

memory device for mutual authentication because, in order to use

good authentication and encryption algorithms, there must be

enough computation power in the device. One of ordinary skill in

the art would have been motivated to do so in order to allow those

memory devices that lack enough support of computation

resources to perform the authentication themselves to still be a

secure part of the system.

Regarding Claim 8,

Claim 8 is a method claim that is substantially equivalent to

apparatus claim 1. Therefore, claim 8 is rejected under a similar

rationale.

Regarding Claim 12,

Claim 12 is a program providing medium claim that is

substantially equivalent to apparatus claim 1. Therefore, claim 12

is rejected under a similar rationale.

Regarding Claim 13,

MGPUB discloses the following:

A data processing apparatus [memory stick walkman] for

recording data to, or reproducing data from, a memory device

[memory stick], comprising:

A controller (Figure 3, CPU);

A memory (Page 4, Paragraph 2 and Figure 11);

Wherein the recording of the data to, or reproducing of the

data from, the memory device is conditioned upon the

establishment of a mutual authentication between the controller and

the memory device (Page 2, Paragraph 1, lines 8-10).

MGPUB does not disclose the use of a virtual memory.

Lin, however, discloses that mutual authentication will take

place between a proxy emulating the memory device and the

controller when the memory device does not support mutual

authentication (Detailed Description, Paragraph 0021, lines 4-14).

This new system would be the system of MGPUB mutually

authenticating the controller with a proxy acting on behalf of the

memory device.

It would have been obvious to one of ordinary skill in the art

at the time of applicant's invention to use a proxy to emulate the

memory device for mutual authentication because, in order to use

good authentication and encryption algorithms, there must be

enough computation power in the device. One of ordinary skill in

the art would have been motivated to do so in order to allow those

memory devices that lack enough support of computation

resources to perform the authentication themselves to still be a

secure part of the system.

Regarding Claim 20,

Claim 20 is a method claim that is substantially equivalent to

apparatus claim 13. Therefore, claim 20 is rejected under a similar

rationale.

Regarding Claim 24,

Claim 24 is a computer-readable medium with software code

claim that is substantially equivalent to apparatus claim 13.

Therefore, claim 24 is rejected under a similar rationale.

4.   Claims 2, 9, 14, and 21 are rejected under 35 U.S.C. 103(a) as being

unpatentable over MGPUB in view of Lin (U.S. Patent Application Publication

2002 0,025,046), further in view of Utsumi (U.S. Patent 6,501,163).

Regarding Claim 2

The system from above does not disclose the fact that the

system first checks whether the memory device is capable of

executing mutual authentication.

Utsumi, however, discloses a system that initially checks

whether the memory device for executing data reproduction or data

recording is capable of executing mutual authentication or not

(Column 13, lines 14-20). Utsumi also discloses the processing of

mutual authentication upon condition that the memory device is capable of executing mutual authentication (Column 10, lines 51-59). This new system would be the system from above verifying whether or not the memory device is capable of executing the mutual authentication.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use the authentication-checking scheme of Utsumi in the system from above in order to obtain information involving copyright protection. One of ordinary skill in the art would have been motivated to do so in order to determine whether or not the memory device is ready for copyright protection (Column 13, lines 21-24).

Regarding Claim 9,

Claim 9 is a method claim that is substantially equivalent to apparatus claim 2. Therefore, claim 9 is rejected under a similar rationale.

Regarding Claim 14,

The system from above does not disclose the system first checking whether the memory device is capable of executing mutual authentication.

Utsumi, however, discloses a system that checks if the memory device supports mutual authentication prior to performing the mutual authentication between the controller and the virtual

memory (Column 13, lines 14-20). Utsumi also discloses the recording of data to, or reproduction of data from, the memory device is conditioned upon the establishment of mutual authentication between the controller and the memory device (Column 10, lines 51-59). This new system would be the system from above verifying whether or not the memory device is capable of executing the mutual authentication.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use the authentication-checking scheme of Utsumi in the system from above in order to obtain information involving copyright protection. One of ordinary skill in the art would have been motivated to do so in order to determine whether or not the memory device is ready for copyright protection (Column 13, lines 21-24).

Regarding Claim 21,

Claim 21 is a method claim that is substantially equivalent to apparatus claim 14. Therefore, claim 21 is rejected under a similar rationale.

5.   Claims 3, 5, 10, 15, 17, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over MGPUB in view of Lin (U.S. Patent Application Publication 2002 0,025,046), further in view of Dondeti et al. (U.S. Patent 6,240,188) and Caronni (U.S. Patent 6,195,751).

Regarding Claim 3,

MGPUB discloses that the mutual authentication is executed by applying a key held within the data processing apparatus ["apple" key] and the other authenticating key held within the memory device ["orange" key] (Page 2, Paragraphs 6 and 7).

The system from above does not disclose a hierarchical key tree structure or an enabling key block.

Dondeti et al., however, disclose a hierarchical key tree structure comprising a variety of keys disposed in correspondence with such roots, nodes, and leaves (Column 3, lines 48-58) on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses [members] as own leaves (Column 3, lines 48-49), wherein the enciphering data comprises upper-rank keys to be enciphered by lower-rank keys (Column 3, line 65 to Column 4, line 5). This new system would be the system from above using the key tree hierarchy from Dondeti et al.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to add the hierarchical key tree structure from Dondeti et al. to the system from above in order to allow for many data processing apparatuses. One of ordinary skill in the art would have been motivated to do so in order to make the

tree scalable for the addition or modification of many processing apparatuses (Column 3, lines 60-63).

The system from above does not disclose an enabling key block.

Caronni, however, discloses a key for authenticating distribution of an enabling key block [key manager database] wherein said authenticating key [TEK (Traffic Encryption Key)] is previously enciphered by such an enabling key block containing an enciphering data for enciphering keys (Column 10, lines 3-23). This new system would be the system from above with the enabling key block and authenticating key from Caronni in use.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use the enabling key block from Caronni in the system from above in order to notify all relevant nodes when a new node is added to the tree. One of ordinary skill in the art would have been motivated to do so in order to allow all nodes to gain the knowledge that a node has been added to the tree (Column 13, lines 22-34).

Regarding Claim 10,

Claim 10 is a method claim that is substantially equivalent to apparatus claim 3. Therefore, claim 10 is rejected under a similar rationale.

Regarding Claim 5,

The system from above does not disclose a version controlling process.

Caronni, however, discloses that the enabling key block distribution authenticating key enciphered and presented by the enabling key block is subject to a version controlling process by way of executing a process for renewing individual versions (Column 1, lines 37-46). This new system would be the system from above using a version controlling process.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a version controlling process in the system from above in order to make the system more secure from an attacker. One of ordinary skill in the art would have been motivated to do so in order to narrow the window of opportunity that an attacker has to use the system without authorization.

Regarding Claim 15,

MGPUB discloses that the mutual authentication is performed between the controller and the virtual memory by applying an authenticating key stored in the memory device ["orange" key] and a key held within the data processing apparatus ["apple" key] (Page 2, Paragraphs 6 and 7).

The system from above does not disclose a hierarchical key tree structure or an enabling key block.

Dondeti et al., however, disclose a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves (Column 3, lines 48-58) of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein the data processing apparatus [member] is associated with one of the leaves of the key tree structure (Column 3, lines 48-49), and wherein the enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys (Column 3, line 65 to Column 4, line 5). This new system would be the system from above using the key tree hierarchy from Dondeti et al.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to add the hierarchical key tree structure from Dondeti et al. to the system from above in order to allow for many data processing apparatuses. One of ordinary skill in the art would have been motivated to do so in order to make the tree scaleable for the addition or modification of many processing apparatuses.

The system from above does not disclose an enabling key block.

Caronni, however, discloses an enabling key block distribution authenticating key [TEK (Traffic Encryption Key)] that is previously enciphered by an enabling key block [key manager database] comprising enciphering data for enciphering keys. This

new system would be the system from above with the enabling key

block and authenticating key from Caronni in use.

It would have been obvious to one of ordinary skill in the art

at the time of applicant's invention to use the enabling key block

from Caronni in the system from above in order to notify all relevant

nodes when a new node is added to the tree. One of ordinary skill

in the art would have been motivated to do so in order to allow all

nodes to gain the knowledge that a node has been added to the

tree (Column 13, lines 22-34).

Regarding Claim 22,

Claim 22 is a method claim that is substantially equivalent to

apparatus claim 15. Therefore, claim 22 is rejected under a similar

rationale.

Regarding Claim 17,

The system from above does not disclose a version

controlling process.

Caronni, however, discloses that the enabling key block

The enabling key block distribution authenticating key

enciphered by the enabling key block is subject to a version

controlling process by way of executing a process for renewing

individual versions on the controller (Column 1, lines 37-46). This

new system would be the system from above using a version

controlling process.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a version controlling process in the system from above in order to make the system more secure from an attacker. One of ordinary skill in the art would have been motivated to do so in order to narrow the window of opportunity that an attacker has to use the system without authorization.

6.   Claims 4, 11, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over MGPUB in view of Lin (U.S. Patent Application Publication 2002 0,025,046), Dondeti et al. (U.S. Patent 6,240,188), and Caronni (U.S. Patent 6,195,751), further in view of Story et al. (U.S. Patent Application Publication 2002 0,046,181) and Traw et al. (U.S. Patent 5,949,877).

Regarding Claim 4,

The system from above does not disclose a licensing system.

Story et al., however, disclose that only a properly licensed data processing apparatus is enabled to decode the enabling key block, whereas such a data processing apparatus devoid of a proper license is unable to decode the enabling key block in a plurality of data processing apparatuses (Detailed Description, Paragraph 41). This new system would be the system from above

using licenses to determine if a data processing apparatus is legal or not.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use licensing in the system from above in order to determine those data processing apparatuses that are able to legally record and output data. One of ordinary skill in the art would have been motivated to do so in order to enable only those devices with a proper license to decrypt and play digital content.

The system from above does not disclose the act of revoking an illegal data processing apparatus.

Traw et al., however, disclose that the data processing apparatus prevents such an improper data processing apparatus devoid of a proper license from illegally implementing anything with the virtual memory device by way of revoking the improper data processing apparatus (Column 3, lines 34-43). This new system would be the system from above revoking illegal data processing apparatuses.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to revoke improper data processing apparatuses in order to maintain access for only those devices that have the correct license. One of ordinary skill in the

art would have been motivated to do so in order to revoke the

license of any device that has been compromised.

Regarding Claim 11,

Claim 11 is a system claim that is substantially equivalent to

apparatus claim 4. Therefore, claim 11 is rejected under a similar

rationale.

7.   Claims 6, 7, 18, and 19 are rejected under 35 U.S.C. 103(a) as being

unpatentable over MGPUB in view of Lin (U.S. Patent Application Publication

2002 0,025,046), further in view of Dondeti et al. (U.S. Patent 6,240,188)

Regarding Claim 6,

The system from above does not disclose a hierarchical key

tree structure.

Dondeti et al., however, disclose the following:

In a key tree structure comprising a variety of keys disposed

in correspondence with roots, nodes, and leaves on such paths

ranging from roots to leaves of the key tree structure (Column 3,

lines 48-58) comprising a plurality of data processing apparatuses

[members] as own leaves (Column 3, lines 48-49),

Those leaf-keys provided in correspondence with own

leaves are respectively enciphered by a storage key proper to the

individual data processing apparatuses and then stored in memory

means inside of the corresponding data processing apparatus

(Column 3, lines 52-56).

This new system would be the system from above using the

key tree hierarchy from Dondeti et al.

It would have been obvious to one of ordinary skill in the art

at the time of applicant's invention to add the hierarchical key tree

structure from Dondeti et al. to the system from above in order to

allow for many data processing apparatuses. One of ordinary skill

in the art would have been motivated to do so in order to make the

tree scalable for the addition or modification of many processing

apparatuses (Column 3, lines 60-63).

Regarding Claim 7,

The system from above does not disclose a hierarchical key

tree structure.

Dondeti et al., however, disclose the following:

In a key tree structure comprising a variety of keys disposed

in correspondence with roots, nodes, and leaves on such paths

ranging from roots to leaves of the key tree structure (Column 3,

lines 48-58) comprising a plurality of data processing apparatuses

[members] as own leaves, based on those leaf-keys provided in

correspondence with own leaves (Column 3, lines 48-51),

A device key block as an assemblage of ciphered keys

comprising mutually different individually enciphered node keys of

plural steps ranging from own leaves up to upper-rank keys of the key tree structure is stored in a memory means inside of the data processing apparatus (Column 3, lines 52-56).

This new system would be the system from above using the key tree hierarchy from Dondeti et al.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to add the hierarchical key tree structure from Dondeti et al. to the system from above in order to allow for many data processing apparatuses. One of ordinary skill in the art would have been motivated to do so in order to make the tree scalable for the addition or modification of many processing apparatuses (Column 3, lines 60-63).

Regarding Claim 18,

The system from above does not disclose a hierarchical key tree structure.

Dondeti et al., however, disclose an enciphered leaf key produced by enciphering a leaf key by a storage key that is associated with the data processing apparatus (Column 3, lines 52-56), wherein the leaf key that is part of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure (Column 3, lines 48-58), and wherein the leaf key is associated with the data

processing apparatus [member] (Column 3, lines 48-49). This new

system would be the system from above using the key tree

hierarchy from Dondeti et al.

It would have been obvious to one of ordinary skill in the art

at the time of applicant's invention to add the hierarchical key tree

structure from Dondeti et al. to the system from above in order to

allow for many data processing apparatuses. One of ordinary skill

in the art would have been motivated to do so in order to make the

tree scaleable for the addition or modification of many processing

apparatuses (Column 3, lines 60-63).

Regarding Claim 19,

The system from above does not disclose a hierarchical key

tree structure.

Dondeti et al., however, disclose a device key block

comprising an assemblage of ciphered keys further comprising

mutually different individually enciphered node keys (Column 3,

lines 52-56) in a hierarchical key tree structure comprising a variety

or keys disposed in correspondence with roots, nodes, and leaves

of the key tree structure on paths ranging from roots to leaves of

the key tree structure (Column 3, lines 48-58), and wherein one of

the leaves is associated with the data processing apparatus

[member] (Column 3, lines 48-49). This new system would be the

system from above using the key tree hierarchy from Dondeti et al.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to add the hierarchical key tree structure from Dondeti et al. to the system from above in order to allow for many data processing apparatuses. One of ordinary skill in the art would have been motivated to do so in order to make the tree scaleable for the addition or modification of many processing apparatuses (Column 3, lines 60-63).

8.   Claims 16 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over MGPUB in view of Lin (U.S. Patent Application Publication 2002 0,025,046), Dondeti et al. (U.S. Patent 6,240,188), and Caronni (U.S. Patent 6,195,751), further in view of Story et al. (U.S. Patent Application Publication 2002 0,046,181).

Regarding Claim 16,

The system from above does not disclose a licensing system.

Story et al., however, disclose that the data processing apparatus is properly licensed if the data processing apparatus is enabled to decode the enabling key block and wherein the data processing apparatus is devoid of proper licensing if unable to decode the enabling key block (Detailed Description, Paragraph 41). This new system would be the system from above using licenses to determine if a data processing apparatus is legal or not.

It would have been obvious to one of ordinary skill in the art

at the time of applicant's invention to use licensing in the system

from above in order to determine those data processing

apparatuses that are able to legally record and output data. One of

ordinary skill in the art would have been motivated to do so in order

to enable only those devices with a proper license to decrypt and

play digital content.

Regarding Claim 23,

Claim 23 is a method claim that is substantially equivalent to

apparatus claim 16. Therefore, claim 23 is rejected under a similar

rationale.

Conclusion

Any inquiry concerning this communication or earlier communications from

the examiner should be directed to Jeffrey D. Popham whose telephone number

is (571)-272-7215. The examiner can normally be reached on M-F 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, Andrew Caldwell can be reached on (571)-272-3868.

The fax phone number for the organization where this application or proceeding

is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free).

Andrew Caldwell